F6

Threat Intelligence

Проактивный анализ киберугроз

F6

1 300+
успешных исследований киберпреступлений по всему миру

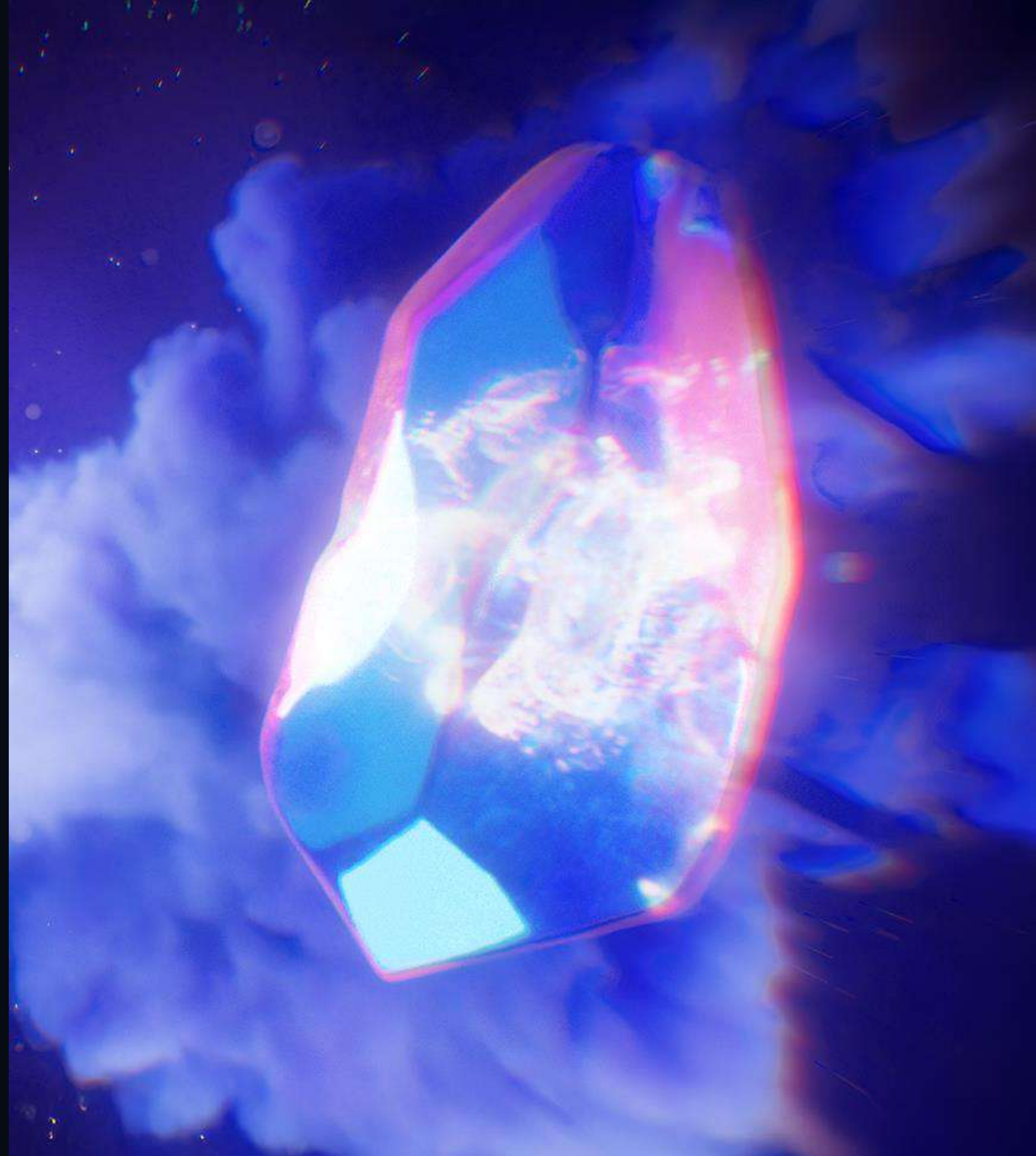
600
enterprise-клиентов

№1
первый поставщик услуги Incident Response в России

120+
патентов и заявок

20 млрд+
рублей сохраняют наши технологии в бюджете клиентов ежегодно

20 лет
практики и уникальной экспертизы на рынке РФ



История F6

F6

- **2003** — Основание компании
- **2011** — Открытие первого в России CERT
- **2013** — Запуск Threat Intelligence
- **2014** — Запуск Threat Hunting Framework
- **2015** — Запуск платформы Fraud Protection
- **2017** — Запуск Digital Risk Protection
- **2021** — Запуск Attack Surface Management; Запуск Business Email Protection
- **2022** — Фонд «Сайберус» приобрел компанию F.A.C.C.T.
- **2024** — Ребрендинг: новое имя в мире кибербезопасности

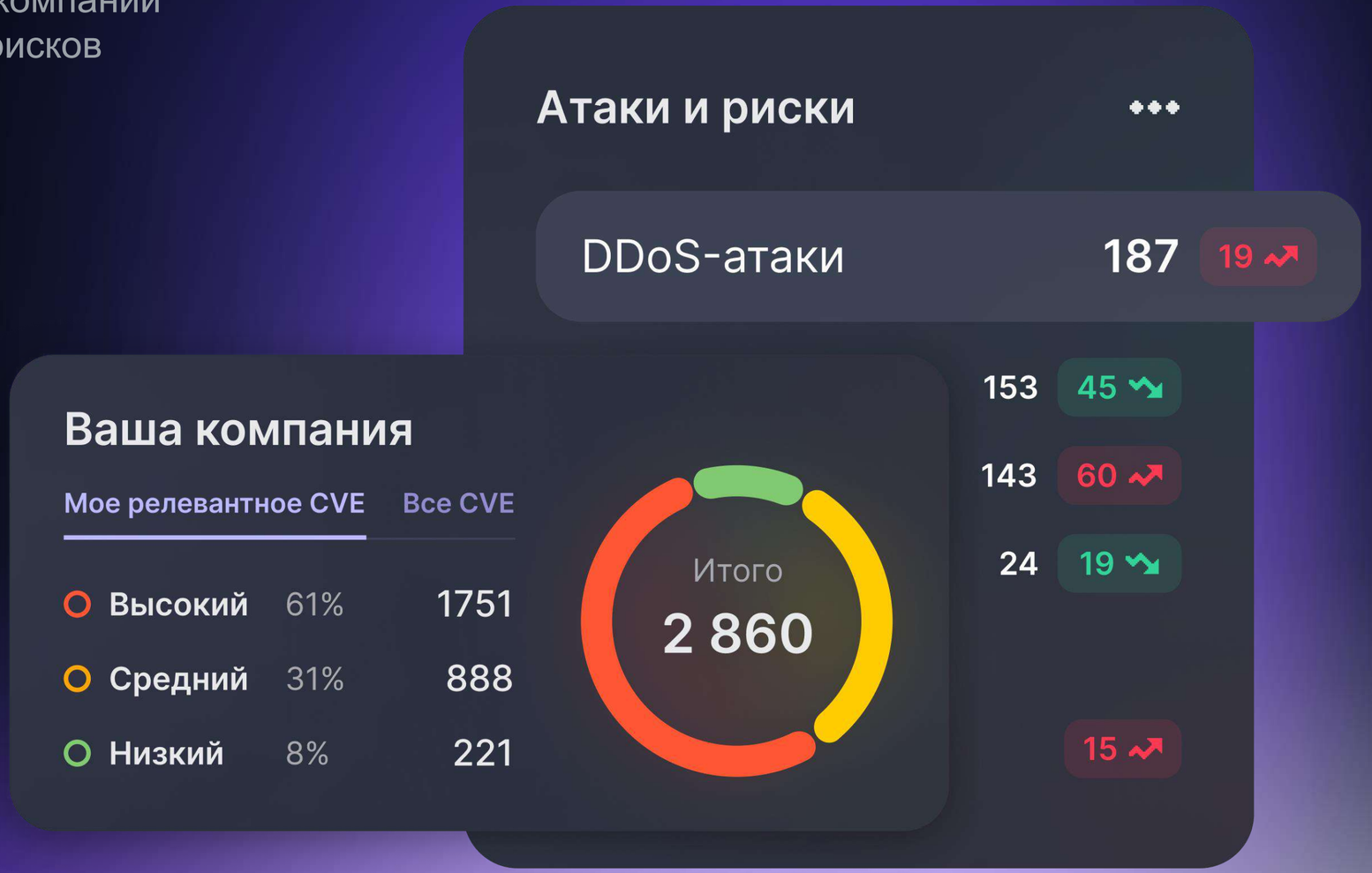
2003-2011 — Компания основана как частное кибердетективное агентство

2013-2025 — Разработка собственных продуктов по кибербезопасности

Threat Intelligence

F6

С Threat Intelligence от F6 вы получаете персонализированную, проверенную и значимую информацию из сотен источников, необходимую для построения эффективной защиты вашей компании от финансовых потерь и репутационных рисков



Threat Intelligence дает ответы на ключевые вопросы безопасности

F6

1. Выдержит ли ваша система безопасности кибератаку?

2. Как, с помощью каких инструментов вас будут атаковать?

3. Какие меры безопасности необходимо применить?

4. Что говорят о вашей компании на хакерских площадках?

5. Как преступники используют или планируют использовать ваш бренд?

Почему важно предотвращать атаки, а не только ликвидировать последствия?

F6

Высокие финансовые издержки

Каждый час простоя обходится компании в среднем до 40 миллионов рублей

Репутационные потери

Утечка данных или сбой в работе систем могут серьезно подорвать доверие клиентов партнеров

Затраты на восстановление

Восстановление после кибератаки может занять до 80 дней и потребовать значительных финансовых ресурсов

Threat Intelligence от F6 предоставляет данные о всех угрозах, направленных на вашу компанию

Интеграция этих данных в вашу систему безопасности позволяет:

Обнаруживать, идентифицировать и приоритизировать угрозы до того как они нанесут ущерб

Получайте информацию о последних угрозах, включая индикаторы компрометации, тактики, техники и процедуры, которые используются злоумышленниками и сокращайте время на обнаружение угроз.

Оценивать ландшафт угроз вашей компании

Threat Intelligence открывает компаниям доступ к аналитическим отчетам об угрозах за пределами их собственных сетей и цифрового присутствия, а также за пределами экспертизы поставщиков решений SIEM.

Оптимизировать защиту вашей организации

Данные Threat Intelligence позволяют принимать обоснованные решения по улучшению политики безопасности и внедрению необходимых защитных мер. Это позволяет компаниям быстрее реагировать на угрозы.

Минимизировать финансовые потери от кибератак

Убытки организаций, использующие атрибутированные данные киберразведки, снижаются на 20-30% в сравнении с компаниями, которые не используют продвинутые решения по управлению угрозами.

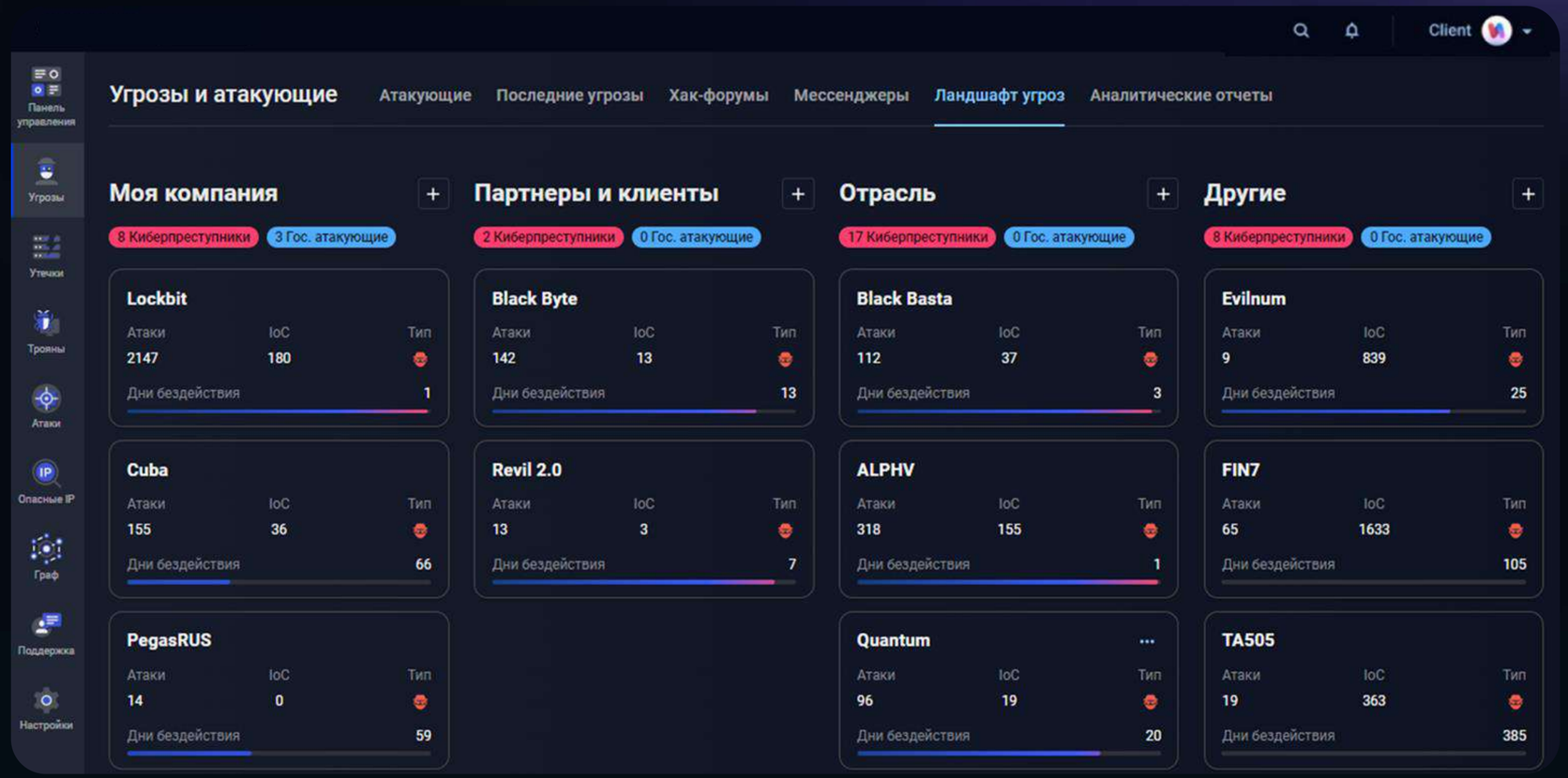
Ключевые возможности Threat Intelligence

F6

- Полный ландшафт угроз
- Сбор данныхиз Darkweb
- Атрибуция угроз
- Утечки данных
- Графовый анализ
- Индикаторы компрометации
- Уязвимости
- Детонация ВПО

Полный ландшафт угроз

Получайте актуальные для вашей компании стратегические данные для оптимизации ИБ-стратегии в виде персонализированного дашборда, ежемесячных рассылок, годовых отчетах о трендах и прогнозах

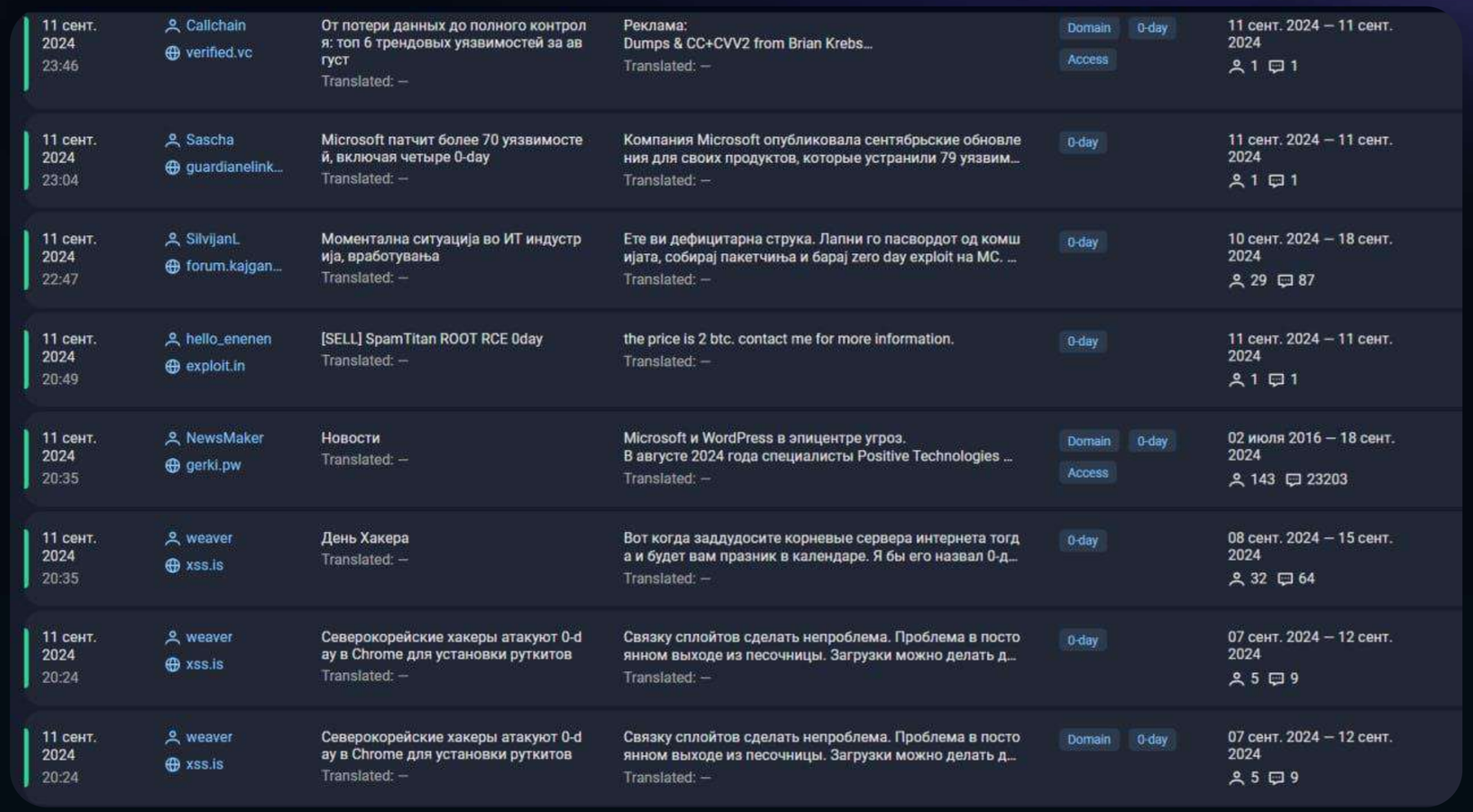


Приоритизируйте задачи по обеспечению безопасности, опираясь данные о нацеленных на организацию злоумышленниках и стратегиях их атак

- Будьте в курсе актуальных угроз для вашей организации, партнеров и отрасли
- Получайте доступ к критически важной информации в один клик
- Изучайте отчеты с прогнозами для проактивного выстраивания стратегии ИБ
- Отслеживайте основные угрозы за выбранный период и развивающиеся тренды угроз

Сбор данных из DarkWeb

F6 собирает самую полную в отрасли базу данных Darkweb. Она включает информацию из закрытых хакерских сообществ, недоступную при использовании стандартных методов, таких как краулеры, скрипты или Big Data



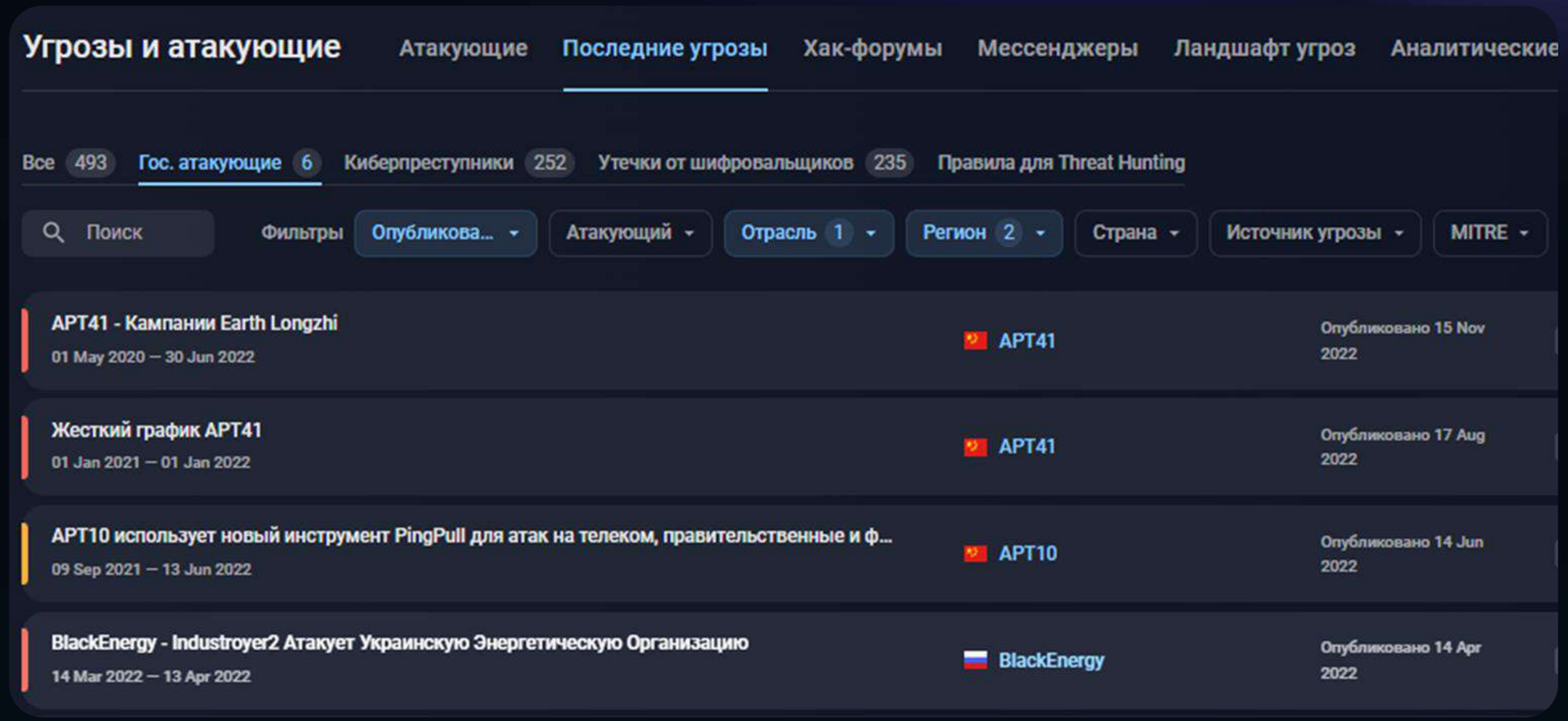
11 сент. 2024 23:46	Callchain verified.vc	От потери данных до полного контроля: топ 6 трендовых уязвимостей за август Translated: –	Реклама: Dumps & CC+CVV2 from Brian Krebs... Translated: –	Domain 0-day Access	11 сент. 2024 – 11 сент. 2024 1 1
11 сент. 2024 23:04	Sascha guardianelink...	Microsoft патчит более 70 уязвимостей, включая четыре 0-day Translated: –	Компания Microsoft опубликовала сентябрьские обновления для своих продуктов, которые устранили 79 уязвим... Translated: –	0-day	11 сент. 2024 – 11 сент. 2024 1 1
11 сент. 2024 22:47	SilvijanL forum.kajgan...	Моментална ситуација во ИТ индустрија, вработувања Translated: –	Ете ви дефицитарна струка. Лапни го пасвордот од комшијата, собирај пакетчиња и барај zero day exploit на МС. ... Translated: –	0-day	10 сент. 2024 – 18 сент. 2024 29 87
11 сент. 2024 20:49	hello_enenen exploit.in	[SELL] SpamTitan ROOT RCE 0day Translated: –	the price is 2 btc. contact me for more information. Translated: –	0-day	11 сент. 2024 – 11 сент. 2024 1 1
11 сент. 2024 20:35	NewsMaker gerki.pw	Новости Translated: –	Microsoft и WordPress в эпицентре угроз. В августе 2024 года специалисты Positive Technologies ... Translated: –	Domain 0-day Access	02 июля 2016 – 18 сент. 2024 143 23203
11 сент. 2024 20:35	weaver xss.is	День Хакера Translated: –	Вот когда заддудосите корневые сервера интернета тогда и будет вам праздник в календаре. Я бы его назвал 0-д... Translated: –	0-day	08 сент. 2024 – 15 сент. 2024 32 64
11 сент. 2024 20:24	weaver xss.is	Северокорейские хакеры атакуют 0-day в Chrome для установки руткитов Translated: –	Связку сплойтов сделать непроблема. Проблема в постоянном выходе из песочницы. Загрузки можно делать д... Translated: –	0-day	07 сент. 2024 – 12 сент. 2024 5 9
11 сент. 2024 20:24	weaver xss.is	Северокорейские хакеры атакуют 0-day в Chrome для установки руткитов Translated: –	Связку сплойтов сделать непроблема. Проблема в постоянном выходе из песочницы. Загрузки можно делать д... Translated: –	Domain 0-day	07 сент. 2024 – 12 сент. 2024 5 9

Выявляйте активность злоумышленников и отслеживайте обсуждения, касающиеся вашей организации

- Новые стратегии атак
- Инсайдерские угрозы
- Изменения тактик и целей
- Продажа скомпрометированных данных
- Профили злоумышленников
- Новое вредоносное ПО и его модификации

Атрибуция угроз

Threat Intelligence от F6 отслеживает активность киберпреступников, хактивистов и прогосударственных атакующих и предоставляет информацию об используемых ими тактиках, техниках и процедурах



F6

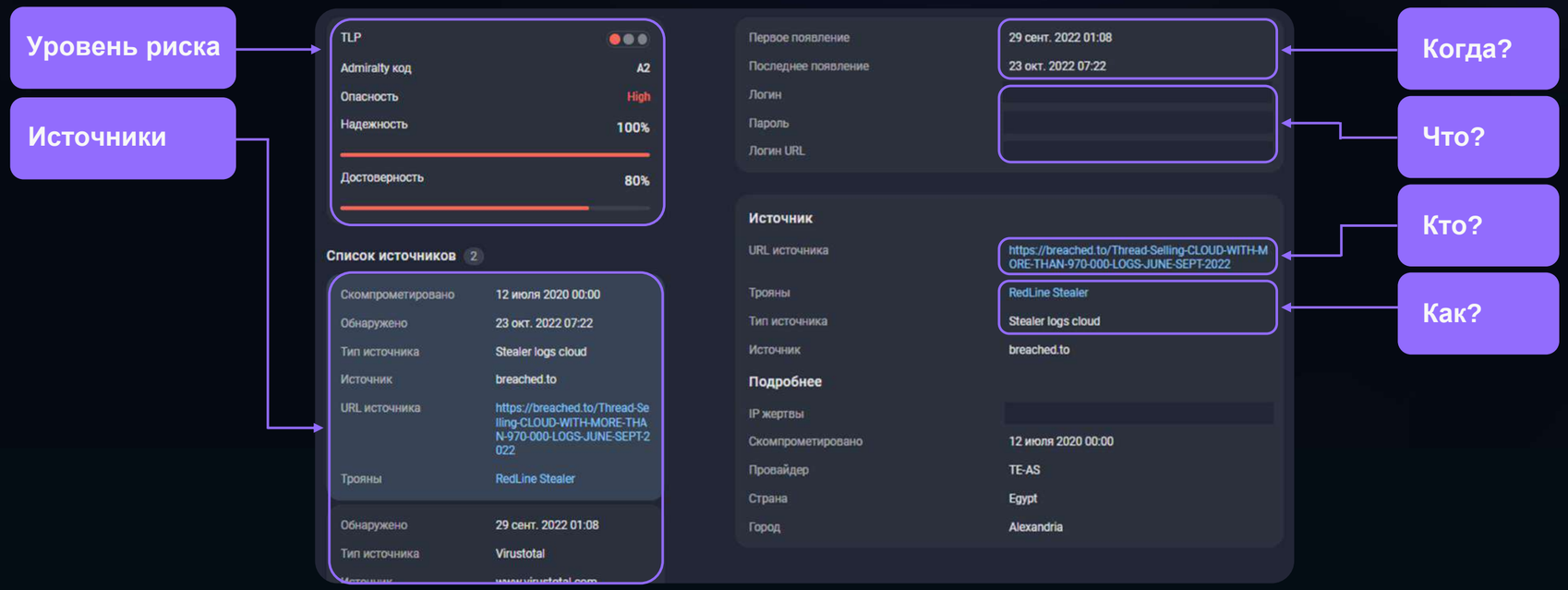
Создавайте правила и фильтры для поиска угроз в режиме реального времени по широкому диапазону атрибутов, включая

- Отрасль жертвы
- Регион жертвы
- Страна жертвы
- Атрибуция атакующих
- Используемые техники по MITRE ATT&CK
- Хронология атаки
- Рекомендации по устранению последствий и снижению рисков от угроз

Утечки данных

F6

Платформа отслеживает информацию об утечках данных, обеспечивая защиту клиентских аккаунтов, VIP-персон и сотрудников организации. Наши источники и методы получения данных киберразведки включают данные с бот-сетей, отслеживание автоматического перевода средств ВПО, мониторинг кардшопов и сервисов проверки скомпрометированных данных, а также информацию из Darkweb



- Логины и пароли клиентов, сотрудников и VIP-персон
- Утекшие данные банковских карт
- Счета, связанные с нелегальным переводом средств
- Взломанные базы данных, опубликованные в Darkweb
- Утечки внутреннего программного кода на GitHub
- Утечки информации в публичных источниках
- Сертификаты и ключи цифровых подписей, потенциально находящиеся под угрозой
- Подробные данные о зараженных конечных точках (в том числе IP-адреса) клиентов, сотрудников и VIP-персон
- Полная хронология событий, относящихся к зараженному устройству

Графовый анализ

F6

Система графового анализа от F6 визуализирует данные киберразведки и выявляет ранее неизвестные связи с помощью запатентованных алгоритмов

Объекты исследования

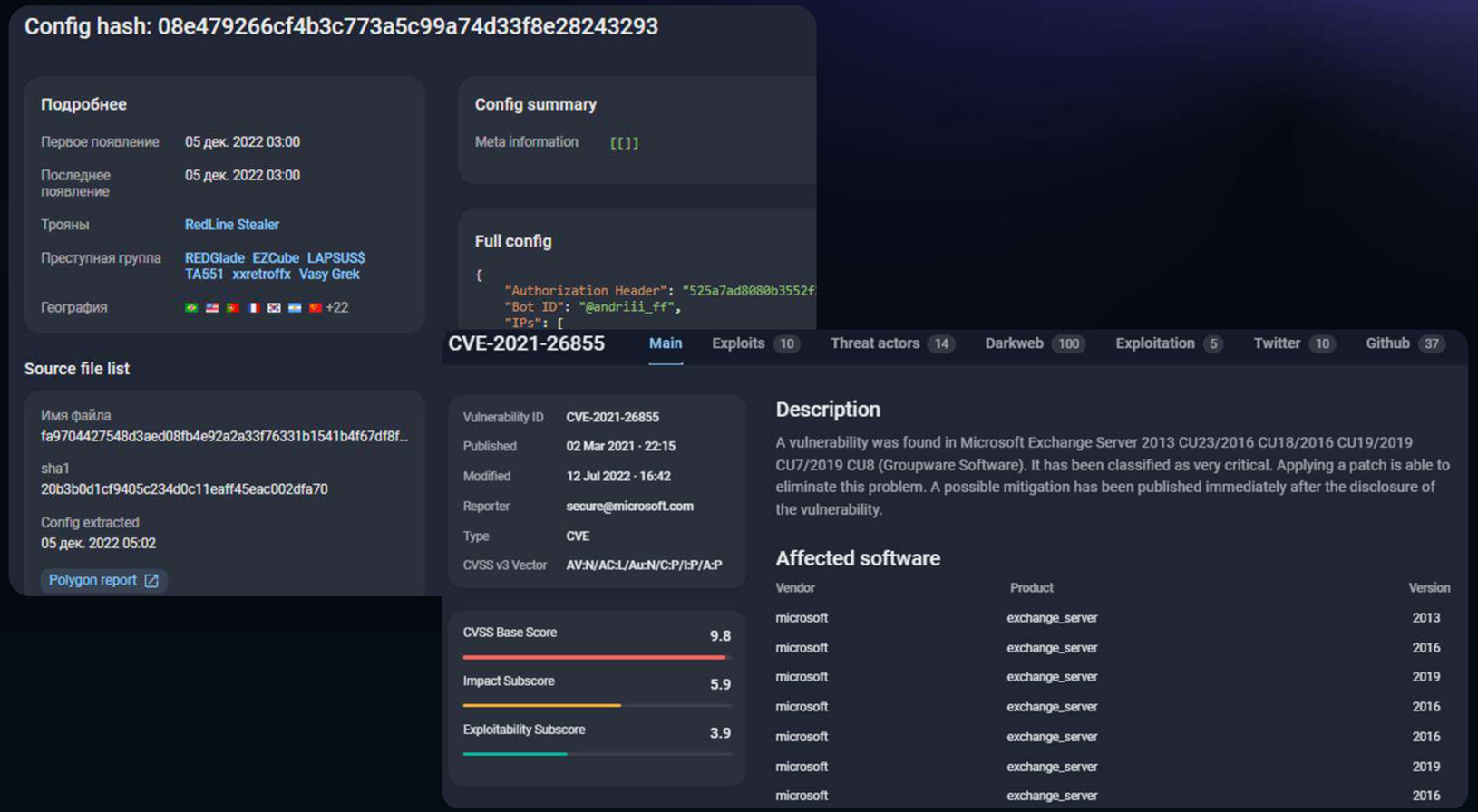
- Регистрационные данные доменов из базы данных WHOIS;
- DNS-записи доменов;
- Данные SSL сертификатов;
- Баннеры и отпечатки сервисов на IP-адресах;
- Скрытые регистрационные данные;
- Бэкенды, спрятанные с помощью прокси-сервисов;
- История регистрационных данных, перемещений по хостингам и изменений сервисов;
- Активность в Darkweb.

Исследуйте связи между атакующими, их инфраструк-турами и инструментами и узнавайте подробную информацию в один клик

- Threat Hunting
- Обогащение индикаторов компрометации
- Корреляция оповещений
- Борьба с фишингом и фродом
- Поиск бэкендов

Данные о ВПО и уязвимостях

Эксперты F6 ежедневно исследуют тысячи вредоносных файлов, собранных в ловушках honeypot, а также полученных в ходе реагирований на инциденты и отслеживания ботнетов



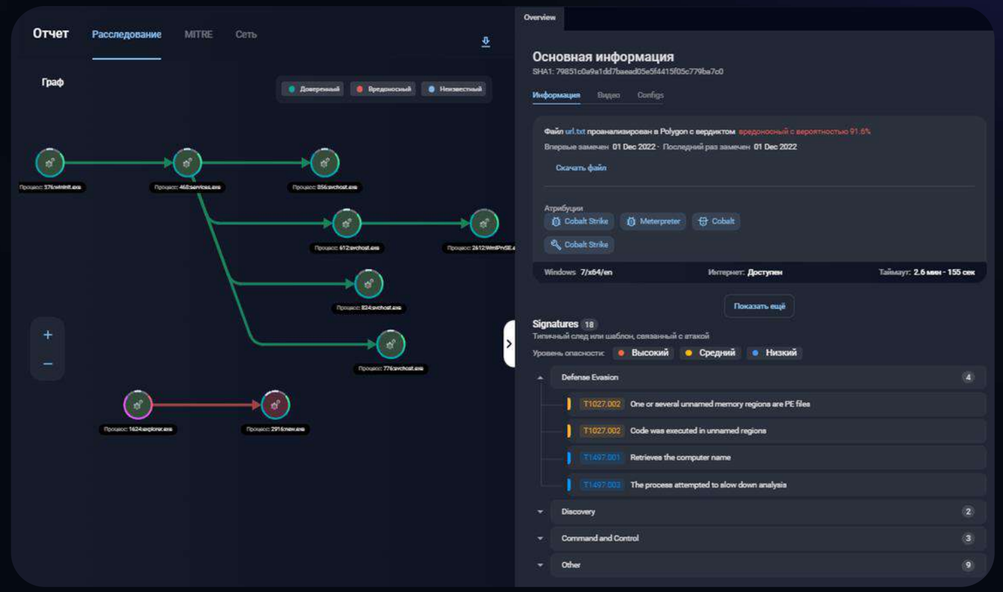
F6

Используйте дашборд для поиска, анализа и приоритизации уязвимостей, на которые нацелено вредоносное ПО. В дашборде вы найдете следующие данные

- Информация о семействах ВПО (включая атрибуцию до преступной группы)
- Информация об актуальных файловых и сетевых индикаторах
- Yara-правила и другие сигнатуры для обнаружения ВПО
- Подробная информация об извлеченных конфигурационных файлах
- Актуальные обновления по уязвимостям и эксплойтам
- Обсуждения эксплойтов на андеграундных форумах и в соцсетях

Детонация ВПО

Подозрительные файлы и ссылки можно отправлять на детальный анализ с помощью платформы детонации F6 или ручной реверс-инжиниринг напрямую из интерфейса **Threat Intelligence**



Глубокий анализ

- Оценка вредоносной активности;
- Поведенческие анализ;
- Сетевая активность;
- Дерево процессов;
- Файловая структура;
- Матрица MITRE ATT&CK;
- Скринкаст действий ВПО.

F6

Собственная платформа детонации ВПО и команда специалистов по реверс-инжинирингу F6 предоставляет следующие возможности:

- Подробные исследования практически любого типа файлов
- Гибкая детонация с настраиваемыми опциями исполнения вредоносного кода
- Анализ заархивированных и защищенных паролем файлов

Гибкая модульная структура

F6

Включенные услуги

- Поддержка*
- Онбородинг
- Неограниченное количество правил для охоты за угрозами
- Неограниченное количество пользователей
- Неограниченный API-доступ
- Поддержка пользовательской интеграции
- Ежемесячные отчеты по Threat Intelligence
- Автоматизированные отчеты

Угрозы

- Киберпреступные группы
- Прогосударственные атакующие
- DLS-сайты вымогательского ВПО
- Ландшафт угроз
- Бюллетени угроз
- Аналитические отчеты
- Открытые угрозы

Утечки

- Скомпрометированные аккаунты
- Публичные утечки
- Git-утечки
- Утечки баз данных
- IMEI

Darkweb

- Андеграундные форумы
- Андеграундные маркетплейсы
- Мессенджеры

Банки

- Скомпрометированные банковские карты
- Данные из кардшопов
- Информация о счетах дропов

Подозрительные IP

- Выходные ноды Tor
- Открытые прокси
- Socks-прокси на ботах
- Сканирующие IP-адреса
- VPN

Трояны

- Отчеты по ВПО
- Детонация ВПО
- Конфигурационные файлы ВПО
- Фишинг-киты
- Уязвимости

Атаки

- DDoS
- Фид подозрительных URL
- Дефейсы

Граф

- Визуализация данных киберразведки с помощью графового анализа

* только «Баги», «Редактирование компании» и «Интеграция»

Источники данных Threat Intelligence

F6

Источники получения данных

- Открытые источники (OSINT)
- Фишинг-киты и ВПО
- Песочницы
- Сетевые СЗИ
- Обсуждения в мессенджерах и на Drakweb-форумах
- DarkWeb-маркетплейсы
- C2-сервера злоумышленников
- Телеметрия сенсоров
- Данные об уязвимостях и эксплойтах

Сбор данных

Граф F6 Threat Intelligence

Визуализация данных и связей

F6 Threat Intelligence

- **Корреляция данных**
- **Определение контекста**
- **Анализ и проверка**
- **Обмен развед данными**
- **Оценка и ранжирование**

Результаты разведки

- Информация об утечках
- Отчеты
- Тренды угроз
- TTPs
- Контекст для команд реагирования
- Выгрузка фидов

Передача данных через API (STIX/TAXII)

Интерфейс F6 Threat Intelligence

Сторонние системы (системы Заказчика)

Компании, интегрировавшие решение Threat Intelligence от F6 отмечают улучшение показателей бизнеса

F6

На 20-30%

снижение убытков по сравнению с теми, кто отказался от получения актуальной киберразведки

На 10-50%

сокращение времени реагирования на инциденты

На 20%

повышение удовлетворенности клиентов за счет стабильной и надежной работы инфраструктуры

F6

Закажите бесплатный пилот прямо сейчас

Всего 1-2 месяца требуется для полной настройки решения
в инфраструктуре организации

F6.ru
info@F6.ru

F6.ru/blog
+7 (495) 984-33-64

Технологии для борьбы с киберугрозами